Congressional Research Service
Informing the legislative debate since 1914

Evolving Electric Power Systems and Cybersecurity

November 4, 2021

Congressional Research Service
https://crsreports.congress.gov
R46959

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46959

November 4, 2021

Richard J. Campbell
Specialist in Energy Policy

Evolving Electric Power Systems and Cybersecurity

Electric power is generated in power plants across the country, and transferred through a network of transmission lines at high voltages to distribution systems, which then bring electric power to the many residential, commercial, and industrial end-users. The transmission system, or the "grid," is the interconnected group of power lines and associated equipment for moving electric energy at high voltage between points of supply and points where it is delivered to other electric systems. The U.S. grid is aging, and one of the tools for modernizing the system is incorporating newer computer systems and devices that allow for automated monitoring and control of the equipment used in the grid.

Cyberattacks are practically a daily occurrence for many U.S. companies and institutions. In this context, cybersecurity has risen as a concern for the integrity and reliability of the grid. Connecting electric power systems to the internet has increased the ability to remotely control the grid, and is largely a result of industry modernization, and the increasing convergence of information technology (IT) and operating technology (OT) systems. IT and OT convergence in the energy industry is leading to common software and security systems use, which may potentially result in increased cybersecurity vulnerability for the grid. Further, the use of older technologies in OT systems may increase cyber vulnerabilities in a converged system due to the challenges companies face in applying patching and system updates to older systems. Companies providing equipment/or services in the supply chain of energy companies have been targets of cyberattacks aimed ultimately at compromising hardware or software to eventually infiltrate energy company networks.

The resources used to provide electric power are changing, as more renewables (particularly wind power and solar photovoltaics) replace fossil fuel sources. As renewable and other resources increase in provision of electricity nationwide, a focus may be how best to secure these resources. Aside from the ability to store electricity produced from renewables at times of off-peak demand, energy storage may also help to stabilize the grid by balancing the grid to maintain system frequency. As utilities begin to deploy larger, longer duration battery systems, the importance of secure renewables and energy storage may become more essential to ensuring the reliability of the grid. Security of these technologies will likely become a part of planning for the future of the grid.

Smart Grid modernization ensues as upgrades to electric power infrastructure are added. Substations controlling transmission voltage are being automated with advanced switching capabilities to enhance current flows and control of the grid. The speed inherent in the Smart Grid's enabling digital technologies may also increase the chances of a successful cyberattack, potentially exceeding the ability of the defensive system and defenders to comprehend the threat and respond appropriately. Machine-to-machine interfaces enabled by artificial intelligence are being investigated to improve cybersecurity.

Various agencies have standards and reporting requirements for reliability, and programs providing "best practices" and cyber and physical security assistance to electric utilities. These agencies include the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation (NERC), and the National Institute of Standards and Technology. Some of these programs provide industry-wide information for companies to act upon, while other programs assist individual companies. The Department of Energy (DOE) also runs the Cybersecurity Risk Information Sharing Program (CRISP) to allow energy sector owners and operators to voluntarily share cyber threat data in near real-time, and help to analyze this data. In 2020, NERC announced that the Electricity Information Sharing and Analysis Center partnered with DOE to expand CRISP to include OT systems with two pilot programs. Additional actions are being taken by utilities to improve security, including the adoption of multi-factor authentication, preparation and practice for potential intrusions, and consideration of best practices from other sectors.

The electric power industry does not have the intelligence-gathering capabilities to deal with the many cyber and physical threats to the grid, many of which appear to come from actors abroad. Instead, the U.S. government analyzes all-source intelligence to understand threats to the energy grid and shares that information with the electricity industry, which applies its expertise to understanding the risks posed to the grid. Government information that is timely and relevant as to the severity of a threat to the grid, and which contains whether a need exists for immediate action, is helpful to the electricity industry. Congress may investigate how best to ensure that intelligence information on grid cyberthreats can be disseminated better and on a timelier basis.

Contents

Introduction 1
Mandatory and Enforceable Critical Infrastructure Protection Standards 2
Grid Security Exercises 3
Electric Grid Threats and Vulnerabilities 3
Operational and Information Technology Systems 4
IT and OT: Increasing Convergence 5
Industrial Control System Vulnerability 6
Grid Timing and the Global Positioning System 8
Greater Electrification of Vehicles 9
Internet of Things 9
Supply Chain Security and Risks 10
Software Vulnerabilities 10
FERC-NERC Supply Chain Standard 11
Executive Orders for Security of Bulk Power System Supply Chain 11
SolarWinds—A Supply Chain Attack 12
Changing Grid Technologies 13
Renewable Energy 13
Energy Storage 14
Cybersecurity of the Smart Grid 15
Federal Actions and Programs to Assist Grid Security 16
Cybersecurity Incident Reporting 16
Cybersecurity Risk Information Sharing Program (CRISP) 16
Cybersecurity Capability Maturity Model 17
NIST Cybersecurity Framework and FERC-NERC CIP Requirements 17
NIST Recommendations and Industry Best Practices 18
Performance Goals for Electric Utilities 19
Improving Cybersecurity of Distribution and Smaller Utilities 20
Additional Actions to Potentially Improve Grid Cybersecurity 20
Multi-Factor Authentication 20
Separate and Independent OT Networks 21
Preparation and Practice for Potential Intrusions 21
Considering Best Practices from Other Sectors 22
117th Congress Legislation 23
Issues for Congress 23

Contacts

Author Information 24

Introduction

Electricity is essentially the lifeblood of the modern, technological society that we enjoy, for without it, the devices and machinery that enable our economy would not be able to function. Electric power is generated in power plants across the country, and transferred through a network of transmission lines at high voltages to distribution systems, which then bring electric power to the many residential, commercial, and industrial end-users.

The *grid* is another name for the transmission system, i.e., the interconnected group of power lines and associated equipment for moving electric energy at high voltage between points of supply and points where it is delivered to other electric systems.[1]

The U.S. grid is aging, and one of the tools for modernizing the system is the incorporation of computerized systems that allow for the rapid monitoring and control of the equipment used in the grid. Connecting these systems to the internet has increased the ability to remotely control aspects of the grid, but this has come with increasing concern for the grid's cybersecurity, as digital systems can be accessed and controlled remotely. The grid also appears to be evolving from a model of central station power plants meant to capitalize on economies of scale, to a more distributed model based on renewable electric power generation. When combined with a growth in internet capable devices (i.e., the Internet of Things), this potentially leads to a growth in entry points and an increasing attack surface for cyberattacks.

Cyberattacks are practically a daily occurrence for many U.S. companies. The motivations of hackers can range from financial gain via blackmail schemes to the acquisition of confidential or proprietary information, with some cyberattacks from nation states probing the grid for weaknesses in order to insert malware.[2] However, according to some sources, cyberattacks are becoming more frequent in the electricity sector.[3] There are reports of hackers shifting their focus from information technology (IT) systems to operating technology (OT) systems at power plants "penetrating as far as the functioning of machines. Instead of spying on data, attackers attempt to interrupt a service or damage critical infrastructures."[4]

Since the 2015 cyberattack in Ukraine,[5] some have expressed increased concern over the cybersecurity of interconnected U.S. electric power systems that constitute the electric grid. The Ukraine cyberattack was against regional distribution electric utilities, and resulted in the loss of

[1] The Energy Information Administration defines the grid as "A system of synchronized power providers and consumers connected by transmission and distribution lines and operated by one or more control centers. In the continental United States, the electric power grid consists of three systems: the Eastern Interconnect, the Western Interconnect, and the Texas Interconnect. In Alaska and Hawaii, several systems encompass areas smaller than the State (e.g., the Interconnect serving Anchorage, Fairbanks, and the Kenai Peninsula; individual islands)." See Energy Information Administration at http://www.eia.gov/tools/glossary/index.cfm.

[2] The National Institute of Standards and Technology defines malware as "Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code." National Institute of Standards—Computer Security Resource Center, *Malware*, p. 2021, https://csrc.nist.gov/glossary/term/malware.

[3] Bloomberg Law, *Biden Rushes to Protect Power Grid as Hacking Threats Grow (1)*, April 14, 2021, https://news.bloomberglaw.com/privacy-and-data-security/biden-rushes-to-protect-the-power-grid-as-hacking-threats-grow.

[4] See Nina Terp, "Cybersecurity in and for Large Transmission Projects," *Power Magazine*, December 2020, pp. 26-27.

[5] Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense Use Case*, March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

electric power to approximately 225,000 customers for several hours. The cyberattack and blackouts demonstrated conclusively that an electric grid could be infiltrated, controlled, and rendered inoperable through internet-connected systems by an outside, unauthorized entity.[6]

This report focuses on the current state of U.S. electric grid security, given recent cybersecurity events. How the grid is evolving with respect to the mandatory and enforceable regulations for bulk system reliability is a key area of the discussion. Some of the known cybersecurity intrusions are reviewed with respect to the grid vulnerabilities. The report identifies and summarizes several 117th Congress measures related to improving electric grid security with regard to the goal of enhancing the reliability of the U.S. electric power system.

Mandatory and Enforceable Critical Infrastructure Protection Standards

The U.S. bulk electric power system has mandatory and enforceable standards for cybersecurity.[7] The Energy Policy Act of 2005 (EPACT) (P.L. 109-58) gave the Federal Energy Regulatory Commission (FERC) authority over the reliability of the grid, with the power to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). Currently, the North American Reliability Corporation (NERC) serves as the ERO. NERC therefore proposes reliability standards for Critical Infrastructure Protection (CIP), which are updated in response to emerging reliability and cybersecurity concerns for the grid.[8]

FERC has authority over wholesale power sales and the transmission of electricity in interstate commerce, while states have authority over retail sales by electric distribution systems. FERC acknowledged that EPACT excluded local distribution systems from its reliability mandate under Section 215 of the Federal Power Act, as not being part of the bulk power system. However, while that definition excluded facilities in Alaska and Hawaii, it also excluded virtually the entire grid in cities with large distribution systems like New York City. FERC approved NERC's revised criteria and new definition of the bulk electric system in 2012.[9] These criteria and definitions apply to all NERC regions and are a bright-line threshold including all transmission elements operated at 100 kilovolts (kV) or higher, and real power and reactive power resources connected at 100 kV or higher.[10]

---

[6] "The cyberattacks in Ukraine are the first publicly acknowledged incidents to result in power outages. As future attacks may occur, it is important to scope the impacts of the incident. Power outages should be measured in scale (number of customers and amount of electricity infrastructure involved) and in duration to full restoration." Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Defense Use Case, March 18, 2016, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[7] FERC Order No. 773 establishes a "bright-line" threshold essentially considering all transmission facilities and related facilities operating at 100 kiloVolts or above to be part of the bulk electric power system. As such, these facilities are subject to the applicable NERC reliability standards.

[8] For further discussion of the nation's critical infrastructure, see CRS Report R45809, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, by Brian E. Humphreys.

[9] See 139 FERC 61,247.

[10] Real (or active) power is the "component of electric power that performs work, typically measured in kilowatts (kW) or megawatts (MW)." See https://www.eia.gov/tools/glossary/index.php?id=R#real_power. Reactive power is the "portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. Reactive power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly

Congress included provisions in the "Fixing America's Surface Transportation Act" (FAST Act; P.L. 114-94) to give the U.S. Department of Energy (DOE) new authority to order electric utilities and NERC to implement emergency security actions.[11] DOE is designated as the lead sector risk management agency for the Energy sector with responsibilities for both physical and cyber security.[12]

Grid Security Exercises

Every two years, NERC organizes a two-day grid security exercise (GridEx) to test the electricity sector's ability to respond to grid security emergencies caused by cyber and physical attacks. Industry stakeholders participate along with FERC, DOE, and other government entities. These GridExs are intended to determine ways to best secure the grid and improve future responses, generally through improved communications among companies and state and federal agencies, and identification of lessons learned. According to NERC, "GridEx V in 2019 included more than 500 electric utilities, government and law enforcement agencies, and other organizations."[13] According to NERC, engaging senior company leadership is a key to ensuring that appropriate company resources are focused on grid security. After each GridEx session, an unclassified report of results and recommendations is made available to the public.

Electric Grid Threats and Vulnerabilities

Cybersecurity has risen as a concern for the integrity and reliability of the grid, largely as a result of the conversion from analog devices operated by switches, levers, and dials, to a digital system run by programmable digital devices on computerized networks. Connecting electric power control systems to the internet is largely a result of industry modernization, and the increasing convergence of IT and OT systems. Internet connection potentially raises the stakes, however, for security intrusions into grid control systems.

According to a 2015 report from the Idaho National Laboratory, there has been a discernable model in cyberattacks against the grid, with known attacks against the energy sector often following "a phased pattern that focuses on discovery, capture, and exfiltration of data, which generally does not produce tangible or immediately detectable consequences. However, if an attacker's goal is to 'degrade, disrupt, deny, [or] destroy' utility operations, prior reconnaissance and established access provide launch points for destructive payloads (malware)."[14]

---

influences electric system voltage. It is a derived value equal to the vector difference between the apparent power and the real power. It is usually expressed as kilovolt-amperes reactive (KVAR) or megavoltampere reactive (MVAR)." See https://www.eia.gov/tools/glossary/index.php?id=R#reactive_power.

[11] Section 61003 of the FAST Act creates a new Section 215A of the Federal Power Act, that following a written determination by the President, authorizes DOE to order utilities, NERC, and regional entities to implement emergency security measures for up to 15 days at a time.

[12] The energy sector is one of 16 critical infrastructure sectors identified in Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience. Sector-specific agencies are designated with specialized expertise in those critical infrastructure sectors that are tasked with various roles and responsibilities for their respective sectors, as specified in PPD-21 (i.e., development of sector-specific plans, coordination with the Department of Homeland Security, and incident management responsibilities).

[13] North American Electric Reliability Corporation, *GridEx*, 2021, https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx.

[14] Idaho National Laboratory—Mission Support Center, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, August 2016, p. 4, https://www.energy.gov/sites/prod/files/2017/01/f34/

Cybersecurity threats can arise from a number of sources, ranging from deliberate cyberattacks by nation states[15] to acts of malice from discontented current or former employees. They also can result from terrorists,[16] industrial spies and organized crime groups,[17] and other groups with hacking capabilities such as hacktivists.[18] However, some observers have asserted that while terrorists (who seek to damage the U.S. economy) may be able to buy the technical capacity for a cyberattack on the grid from hacktivists, they would be more likely to seek an attack causing direct physical destruction.

Operational and Information Technology Systems

Many electric utilities rely on several different business units for generation, transmission and distribution of energy. Electric and gas utilities often operate this infrastructure over service territories that can be spread across many sites. Such a widespread distribution of facilities complicates the task of monitoring IT and OT systems, and securing the facilities from unauthorized entry or sabotage.[19]

IT systems generally use a binary digital format (i.e., a string of zeroes or ones) in a networked computer environment for data collection, processing, and storage over the Internet. IT systems are the basis of the information that utilities use for applications such as customer billing, and corporate communications.

Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

[15] "National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures. The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures. Their goal is to weaken, disrupt or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the US economy, full scale attack of the infrastructure when attacked by the U.S. to damage the ability of the US to continue its attacks." Industrial Control Systems Cyber Emergency Response Team, *Cyber Threat Source Descriptions*, 2016, https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions. (Hereinafter, ICST).

[16] "Traditional terrorist adversaries of the U.S., despite their intentions to damage U.S. interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries. They are likely, therefore, to pose only a limited cyber threat. Since bombs still work better than bytes, terrorists are likely to stay focused on traditional attack methods in the near term. We anticipate more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks. Their goal is to spread terror throughout the U.S. civilian population. Their sub-goals include: attacks to cause 50,000 or more casualties within the U.S. and attacks to weaken the U.S. economy to detract from the Global War on Terror." ICST.

[17] "International corporate spies and organized crime organizations pose a medium-level threat to the US through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent. Their goals are profit based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry using potential public exposure as a threat." ICST.

[18] "Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-U.S. motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause." ICST.

[19] Tucker Bailey, Adam Maruyama, and Daniel Wallance, "The Energy-Sector Threat: How to Address Cybersecurity Vulnerabilities," *Power Magazine*, October 9, 2020, https://www.powermag.com/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities/.

OT systems are generally those systems and technologies used in power generation, remote control of devices via industrial control systems (ICS), and supervisory control and data acquisition (SCADA). Historically, these functions were largely controlled by analog circuits with varying magnitudes of electronic pulses to control systems.[20] The use of networked computers connected over the internet for OT systems is a relatively new application. The separation from internet-connected systems (i.e. air gapping) provided a certain measure of security for OT systems due to their isolation. But air-gapped systems can be overcome, as was demonstrated by the Stuxnet malware.

> The oft-cited solution of an air-gap between critical systems, or physically isolating a secure network from the internet, was precisely what the Stuxnet worm was designed to defeat. The worm was specifically created to hunt for predetermined network pathways, such as someone using a thumb drive, that would allow the malware to move from an internet-connected system to the critical system on the other side of the air-gap.[21]

IT and OT: Increasing Convergence

IT and OT convergence in the energy industry is leading to common software and security systems use, which may potentially result in increased cybersecurity vulnerability for the grid. While IT and OT systems at utilities have traditionally been independent systems, improvements in technology and expectations of increased efficiency have been leading to a convergence of the two systems.

> In today's world of connectivity and real-time data, bridging the gap between IT and OT systems creates new opportunities to improve operational efficiency, meet customer demands, and keep pace with digital transformation. With enterprise applications (IT) and operations running the grid (OT) working together, utilities can benefit from disaster recovery and business continuity efforts. The integration of these systems enables an organization to optimize data consistency and management, which increases productivity and other efficiencies including network planning and engineering, service assurance, and service fulfillment.[22]

According to the Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA),

> OT components are often connected to information technology (IT) networks, providing a path for cyber actors to pivot from IT to OT networks. Given the importance of critical infrastructure to national security and America's way of life, accessible OT assets are an attractive target for malicious cyber actors seeking to disrupt critical infrastructure for profit or to further other objectives. As demonstrated by recent cyber incidents, intrusions affecting IT networks can also affect critical operational processes even if the intrusion does not directly impact an OT network.[23]

---

[20] Nisarg Desai, *IT vs. OT for the Industrial Internet—Two Sides of the Same Coin?*, April 27, 2016, https://www.globalsign.com/en/blog/it-vs-ot-industrial-internet.

[21] Michael McElfresh, "Can the Power Grid Survive a Cyberattack?," *TheConversation*, June 8, 2015, https://theconversation.com/can-the-power-grid-survive-a-cyberattack-42295.

[22] Ulrich Schälling, *How to Achieve IT and OT Convergence with Unified Management*, Smart Energy International, April 3, 2020, https://fntsoftware.com/blog/industry-expertise-how-to-achieve-it-and-ot-convergence/.

[23] Cybersecurity and Infrastructure Security Agency, *Rising Ransomware Threat to Operational Technology Assets*, June 2021, https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf.

With the increasing use of digital systems, processes in IT and OT are able to use "the same infrastructure components and applications. Smart metering is an example of this. The meters themselves are OT and are a part of the electricity distribution network, yet the meter data management and back office functions are classic IT applications."[24]

The use of software applications to enable easier monitoring and access to OT systems could increase risks.

> For example, some OT policy regimes may allow the use of untested Internet of Things (IoT) technology and even makeshift technical solutions to monitor operations without considering larger-scale cyber vulnerabilities. One regional utility we visited relied on smartphones running a videoconferencing app to monitor the pilot flame in an oil refinery. Combined with the large number of employees, contractors, and vendors who require access to utility company sites and systems, these organizational gaps make IT security policies, including identity and access management (IAM), especially difficult.[25]

The use of use older technologies in OT systems may present an increased potential for cyber vulnerabilities in a converged system.

> [M]any OT systems run on legacy technology that is serviceable only by one or two vendors. These vendors frequently do not prioritize security and may introduce attack vectors by using unpatched laptops and improvised solutions such as USB-based file transfers across separate utility companies. In some cases, utilities that want vendors to use "clean," patched laptops for OT maintenance are required to provide this equipment to vendors at their own expense. When breaches in legacy OT hardware occur, response time is frequently lengthened by a dependency on vendor timetables, an inability to leverage crowdsourced solutions such as cloud detection, and the need to create new solutions for hacks targeted against specific OT systems and configurations.[26]

Industrial Control System Vulnerability

The electric grid relies on a number of electronic devices, switches, and circuit breakers to regulate and report on the flow of electricity at different parts of the system. Together, these pieces of mechanical and automated equipment constitute the grid's ICS network, managing power plant controls, transformer yard and power bus functions, transmission, and distribution substations. The grid's ICS networks essentially operate in a "control loop" in which sensors continually check key components, with variable responses against control variables to ensure that the system is functioning as designed. ICS networks control industrial processes in a number of energy and manufacturing operations.[27]

In October 2020, CISA issued a report warning of existing software vulnerabilities in the electric grid.[28] The alert said that nation-state hackers routinely target ICSs accessed via the internet. According to DHS, internet-accessible OT assets are becoming more prevalent across the 16 U.S.

---

[24] Ulrich Schälling, *Bridging the Gap Between IT and OT Systems*, Smart Energy International, January 8, 2020, https://www.power-grid.com/td/bridging-the-gap-between-it-and-ot-systems/.

[25] Tucker Bailey, Adam Maruyama, and Daniel Wallance, *The Energy-Sector Threat: How to Address Cybersecurity Vulnerabilities*, McKinsey and Company, November 3, 2020, https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities#.

[26] Ibid.

[27] CRS Report R45312, *Electric Grid Cybersecurity*, by Richard J. Campbell.

[28] DHS-CISA, *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems*, October 24, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-205a.

critical infrastructure sectors as companies increase remote operations and monitoring, accommodate a decentralized workforce, and expand outsourcing of key skill areas such as instrumentation and control, OT asset management/maintenance, and, in some cases, process operations and maintenance. Legacy OT assets (i.e., those that were not designed to defend against malicious cyber activities), combined with readily available information that identifies OT assets connected via the internet are "creating a 'perfect storm' of 1) easy access to unsecured assets, 2) use of common, open-source information about devices, and 3) an extensive list of exploits deployable via common exploit frameworks."[29]

CISA described potential cyber threat types and actors that operators of ICS should be aware of in their efforts to secure the grid. While the list of threats could be generally targeted against any part of critical infrastructure, the list is intended to focus on the need "to create a secure cyber-barrier around the Industrial Control System."[30] Cyber threats to a control system refer to "persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet."[31]

A 2020 report from Claroty, a firm specializing in OT security, analyzed 365 ICS vulnerabilities published by the National Vulnerability Database, and 139 ICS advisories issued by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) during the first-half of 2020. The report indicated that this represented a 10.3% increase in software vulnerability disclosures compared to last year; more than 75% of vulnerabilities were assigned high or critical vulnerability scores.[32]

In the first half of 2021, Claroty reported that it found more than 637 vulnerabilities affecting ICS products, affecting products sold by 76 vendors.[33] The report from Claroty compared this finding to numbers from the second half of 2020, in which "449 vulnerabilities were disclosed, affecting 59 vendors. 70.93% of the vulnerabilities are classified as high or critical," which was estimated to be about the same as the second half of 2020.[34] Claroty observed that 61.38% of these flaws could be remotely exploitable vulnerabilities, potentially enabling attacks "from outside the IT or OT network."[35]

Most of the vulnerabilities reported were described as impacting products on the operations management level, followed by basic programmable control and similar devices, and supervisory control devices.

[29] Ibid.

[30] CISA, *Cyber Threat Source Descriptions*, 2021, https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions.

[31] Threats to control systems can come from numerous sources, including national governments, terrorist groups, international corporate spies, and organized crime organizations, hacktivists, and hackers. These are all described further on this webpage. CISA, *Cyber Threat Source Descriptions*, 2021, https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions.

[32] Claroty, *Remotely Exploitable ICS Vulnerabilities on Rise, as Reliance on Remote Access to Industrial Networks Increases During COVID-19*, August 19, 2020, https://www.claroty.com/resource/remotely-exploitable-ics-vulnerabilities-on-rise-as-reliance-on-remote-access-to-industrial-networks-increases-during-covid-19/.

[33] Claroty, *Claroty Biannual ICS and Vulnerability 1H:2021*, 2021, https://claroty.com/wp-content/uploads/2021/08/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H_2021.pdf.

[34] Ibid., p.3.

[35] Ibid, p. 5.

Grid Timing and the Global Positioning System

Much of the ICS and grid function relies on accurate time signals provided by the satellite global positioning system (GPS). These signals are used by grid devices (such as phasor measurement units (PMUs))[36] to enable the synchronization and efficient transmission and distribution of electricity, reporting almost instantaneously on the state of the system. GPSs use an atomic clock[37] to provide a very accurate time signal to devices.

The electric grid uses GPS time signals for accurate synchronization of real-time reporting on the state of the system. Unencrypted GPS signals used in civilian (i.e., non-Defense Department) applications are "easy to capture, process and generate," and "it is not difficult to find a device which can receive and transmit signals in GPS civilian frequency."[38] As a result, GPS spoofing attacks can potentially provide a false time by broadcasting a fake signal, and a "large time error at the phasor measurement units may have serious consequences, including a black-out."[39]

According to one observer, "PMUs are vulnerable to GPS spoofing attacks, wherein a hacker would place transmitters near a station to broadcast counterfeit GPS signals, which would be picked up by the PMUs. Fooling the PMUs of one or more power stations could lead to disruptions that could cascade throughout an entire power grid."[40]

The grid is being modernized as upgrades to electric power infrastructure are added, resulting in what is called the "Smart Grid" as devices capable of two-way communications are added to enhance system monitoring and control. Given the increasing dependence of the digital grid on Smart Grid devices,[41] spoofing attacks that focus on time information at the receiver side may be potentially serious threats to the grid.[42]

A possible defense to GPS spoofing has been proposed using algorithms that analyze previous data that PMUs generated, comparing past to current data. Scientists reported that "their algorithms could detect GPS spoofing attacks and help power grids run even if these attacks compromised up to a third of their nodes."[43] The consistency of data reported across the whole network of PMUs was seen as key to the usefulness of this approach.[44]

---

[36] "Synchrophasors provide a real-time snapshot of current and voltage amplitudes and phases across a power system, and so can give a complete picture of the state of a power system at any instant in time. This makes synchrophasors useful for control, measurement, and analysis of the power system." Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler, "Going Up Against Time: The Power Grid's Vulnerability to GPS Spoofing Attacks," *GPS World*, August 1, 2012, https://www.gpsworld.com/wirelessinfrastructuregoing-against-time-13278/.

[37] "Atomic clocks combine a quartz crystal oscillator with an ensemble of atoms to achieve greater stability. NASA's Deep Space Atomic Clock will be off by less than a nanosecond after four days and less than a microsecond (one millionth of a second) after 10 years. This is equivalent to being off by only one second every 10 million years." See https://www.nasa.gov/feature/jpl/what-is-an-atomic-clock.

[38] Xiao Wei and Biplab Sikdar, *Impact of GPS Time Spoofing Attacks on Cyber Physical Systems*, Institute of Electrical and Electronics Engineers, July 4, 2019, https://ieeexplore.ieee.org/document/8755016.

[39] Ibid.

[40] Charles Q. Choi, *Algorithms Help Power Grids Survive GPS Spoofs*, IEEE, August 7, 2018, https://spectrum.ieee.org/energywise/energy/the-smarter-grid/gps-spoof.

[41] CRS Report R45156, *The Smart Grid: Status and Outlook*, by Richard J. Campbell.

[42] Mehmet Özgün Demir, Güneş Karabulut Kurt, and Ali Emre Pusane, *On the Limitations of GPS Time-Spoofing Attacks*, IEEE, August 11, 2020, https://ieeexplore.ieee.org/document/9163444.

[43] Charles Q. Choi, *Algorithms Help Power Grids Survive GPS Spoofs*, IEEE, August 7, 2018, https://spectrum.ieee.org/energywise/energy/the-smarter-grid/gps-spoof.

[44] For further information on this topic, see Executive Order 13905 "Strengthening National Resilience Through

Greater Electrification of Vehicles

To mitigate potential climate change impacts, some have advocated a greater electrification of the economy to reduce fossil fuel use. Others have voiced concerns over the timing and potential cost of a green energy regime.[45] According to Resources for the Future, "electrification refers to the process of replacing technologies that use fossil fuels (e.g., coal, oil, and natural gas) with technologies that use electricity as a source of energy."[46]

> Depending on the resources used to generate electricity, electrification can potentially reduce carbon dioxide (CO_2) emissions from the transportation, building, and industrial sectors, which account for 63 percent of all US greenhouse gas emissions. Addressing emissions from these sectors is critical to decarbonizing the economy and, ultimately, mitigating the impacts of climate change.[47]

A major opportunity to mitigate climate change could come from electrification of the transportation sector, since most light-duty vehicles (like cars, sport utility vehicles, and small trucks) run on gasoline while heavy-duty vehicles (like buses or large trucks) typically run on diesel fuel. Electrification of transportation, with electric vehicles replacing fossil-fueled vehicles, could lead to a regional or national electric charging infrastructure for these vehicles.

However, charging station infrastructure connections to the grid would have to be secured at the distribution system level to prevent a cyberattacker from taking over the charging system. Electric vehicle charging could present an opportunity for a demand-side attack vector on power grids. One potential scenario for a cyberattack through a grid-connected electric vehicle charging system could cause voltage and frequency instability in the power grid, perhaps leading to cascading failures.[48]

A demand-side cyberattack also could provide false information to grid operators, potentially destabilizing the grid, as the system needs to keep power generated and power used in balance to maintain system frequency and not damage equipment.[49]

Internet of Things

On another level, the growth of internet-capable consumer devices, collectively called *Internet of Things* (IoT), has implications for electric grid cybersecurity as increasing numbers of devices are deployed. IoT devices include internet-connected thermostats and smart inverters on residential

---

Responsible Use of Positioning, Navigation, and Timing Services," 85 *Federal Register* 9359, February 12, 2020, https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing.

[45] Institute of Energy Research, *Cost of Transitioning to 100-Percent Renewable Energy*, July 15, 2019, https://www.instituteforenergyresearch.org/renewable/cost-of-transitioning-to-100-percent-renewable-energy/.

[46] Resources for the Future, *Electrification 101*, December 5, 2019, https://www.rff.org/publications/explainers/electrification-101/.

[47] Ibid.

[48] Samrat Acharya, et al., "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," *IEEE Access*, vol. 8, December 10, 2020, p. 214450.

[49] "Cyber-enabled Demand Side Management (DSM) plays a crucial role in smart grid by providing automated decision-making capabilities that selectively schedule loads on these local grids to improve power balance and grid stability. Security and reliability of the cyber infrastructure that enables DSM is therefore critical to ensuring reliability and safety in energy delivery systems." See Jiyun Lao, *Cybersecurity of Demand Side Management in the Smart Electricity Grid*, 2017, https://preserve.lib.lehigh.edu/islandora/object/preserve%3Abp-11961318.

solar systems. Some of these devices (such as Smart Meters measuring customer electricity use) may be directly connected to OT systems.

Some IoT devices have built-in localized computing capabilities for processing real-time data at the source, which allows these devices to "analyze time-sensitive manufacturing process data and return insights quickly for direct monitoring of industrial conditions" without sending data back to the OT system.[50] These *edge computing* devices are often "responsible for critical industrial systems, that, if shut down or interrupted, would incur severe consequences."[51]

Supply Chain Security and Risks

Companies providing equipment or services in the supply chain of energy companies have been targets of cyberattacks aimed ultimately at compromising hardware or software to eventually infiltrate energy company networks. Supplier companies are possibly targeted as their networks and products may not be as rigorously protected as their energy clients', especially if these clients are bulk power companies.

> Should cyber perimeter defenses be too strong, an attacker could still access the system via the supply chain. For example, the attacker could compromise software updates of either the IT or OT systems and achieve the desired goal when the utility either unwittingly uploads the malignant code into its system or the infected code is uploaded by an insider. A more capable actor could introduce malignant firmware into components—a back door—commonly used in the electricity grid for exploitation at a later date. This equipment compromise can occur during the design, manufacturing, or shipping stages.[52]

Most of the smart meter, sensor, and other equipment makers are international companies who obtain their components from multinational sources, with Taiwan, Singapore, China, and South Korea among the largest manufacturers of semiconductors and microprocessors for smart devices. The opportunity for compromise of equipment made outside of the United States may potentially be greater than for domestic equipment. FERC and NERC are considering how to best manage the risks to the electric grid from the equipment supply chain.[53]

Software Vulnerabilities

Cybersecurity concerns have existed for a number of years regarding software in grid equipment that could lead to cyber vulnerabilities. Many system components use microprocessors or contain specific software programming to function, and may also have control and communications capabilities over remote networks.[54]

---

[50] Stephen Bigelow, Ben Lutkevich, "What Is IT/OT Convergence? Everything You Need to Know," TechTarget, 2020, https://searchitoperations.techtarget.com/definition/IT-OT-convergence.

[51] Ibid.

[52] Office of the Director of National Intelligence, Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions, Public-Private Analytic Exchange Program, 2017, https://www.odni.gov/files/PE/Documents/11—Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf.

[53] 156 FERC ¶ 61,050.

[54] Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, INL/EXT-16-40692, August 2016, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

> The software supporting ICS equipment used in all segments of the power grid in IT and OT environments must also be regularly updated, though doing so sometimes requires system downtime. Scheduled outages of some facilities require approvals and coordinated operational planning activities, as well as potential financial losses associated with outages. To ensure safety and reliability, some utilities, depending on their specific operating environment, may schedule regular (although infrequent) shutdown times coordinated with maintenance windows to conduct updates, as opposed to conducting updates when vulnerabilities emerge. Software can be exploited based on well-known vulnerabilities that remain unpatched, sometimes for years. Most ICS operators rely on vendor-validated patches to be delivered on a regular schedule.[55]

Cyber attackers have been known to take advantage of the tardiness by some energy companies in applying software updates and patches for problems that may be several years old. According to one report, only about 55% of utilities responding to a survey said that they are "utilizing systematic and prompt patching for existing systems."[56] Older, legacy systems may also be a supply chain risk as upgrades and repairs of equipment may not include the installation of up-to-date, security-focused patches.

FERC-NERC Supply Chain Standard

FERC and NERC are looking at the potential to establish a guide to help the electric sector identify vendors of components on their networks so that they can take any necessary action to mitigate potential risks to the bulk power system.

> FERC and NERC have long been focused on supply chain issues, including the development of standards, alerts and other efforts. Supply chain risk management is critical to the reliable operation of the electric grid. FERC and NERC will continue to work together toward assuring the reliability and security of the North American bulk power system.[57]

The agencies also issued a joint white paper to "provide example approaches on assessing infrastructure and the deployment of foreign adversary components that could be used to impact the BPS [bulk power system]."[58]

Executive Orders for Security of Bulk Power System Supply Chain

President Trump issued Executive Order (E.O.) 13920, "Securing the United States Bulk-Power System," in May 2020. In the E.O., the President "declared a national emergency with respect to the threat" to the U.S. bulk-power system, with the goal of limiting the acquisition or use of "equipment designed, developed, manufactured, or supplied by" entities subject to the control of foreign adversaries.[59] The EO directed DOE to establish criteria for pre-qualified vendors and

---

[55] Ibid.

[56] Robert Walton, *State of the Electric Utility 2021: Utilities' Cybersecurity Approach Shows Cause for Concern, Experts Say*, UtilityDive, April 1, 2021, https://www.utilitydive.com/news/state-of-the-electric-utility-2021-utilities-cybersecurity-approach-shows/596664/.

[57] FERC-NERC, *FERC, NERC Publish Guide to Identify Supply Chain Vendors*, July 31, 2020, https://www.nerc.com/news/Headlines%20DL/FERC_NERCSupplyChainWhitePaper_31JULY20.pdf.

[58] FERC-NERC, *Joint Staff White Paper on Supply Chain Vendor Identification—Noninvasive Network Interface Controller*, July 31, 2020, https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf.

[59] Executive Order 13920, "Securing the United States Bulk-Power System," *Public Papers of the Presidents of the United States: Donald R, Trump*, vol. 85 (Washington: GPO, 2020), pp. 44061-44062.

equipment suppliers to the bulk power system, while identifying any now-prohibited equipment currently in use with a goal of isolating, monitoring or replacing such equipment.[60] The issuance of the E.O. reflected the growing focus of the federal government on supply chain risks to the bulk power system.

In December 2020, DOE issued a "Prohibition Order" that prohibited the acquisition, importation, transfer, or installation of specified bulk-power system electric equipment from the Peoples Republic of China, which directly serves Critical Defense Facilities.[61] The Biden administration suspended E.O. 13920 and the Prohibition Order for 90 days in January 2021. In April 2021, the suspension of E.O. 13920 ended, and the DOE Prohibition Order was revoked.

In February 2021, President Biden issued a new Executive Order, E.O. 14107, "America's Supply Chains." Among other provisions, the E.O. directed DOE to identify and make recommendations to address risks in the supply chain for high-capacity batteries and, within one year, to review and make recommendations to improve supply chains for the energy sector industrial base.[62]

DOE followed E.O. 14107 with a Request for Information seeking input from "electric utilities, academia, research laboratories, government agencies, and other stakeholders on various aspects of the electric infrastructure" for a long-term strategy for supply chain security in U.S. energy systems.[63] DOE also announced a 100-day initiative to "enhance the cybersecurity of electric utilities industrial systems and secure the energy sector supply chain."[64] The announcement indicated that DOE will coordinate the supply chain initiative, which is intended to enhance the security of facilities, networks, and software systems with electric utilities and CISA.

SolarWinds—A Supply Chain Attack

SolarWinds is a U.S. company providing software to manage government and private company IT and network systems.[65] According to a report, SolarWinds' Orion product, used by many companies and organizations to provide centralized monitoring and management of various IT systems, was compromised by hackers, who added malicious code (i.e., malware) into Orion's software system.[66] The malware[67] was reported to have "created a backdoor to customer's

[60] CRS Insight IN11417, *E.O. 13920 and Bulk-Power System Supply Chain Security*, by Richard J. Campbell.

[61] Department of Energy, "Prohibition Order Securing Critical Defense Facilities," 86 *Federal Register* 533-536, January 6, 2021.

[62] Executive Order 14107, "America's Supply Chains," *Public Papers of the Presidents of the United States: Joseph R. Biden*, vol. 86 (Washington: GPO, 2021), pp. 11849-11854.

[63] Department of Energy, Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure, 6450-01-P, April 2021, https://www.energy.gov/sites/default/files/2021-04/RFI%20Ensuring%20the%20Continued%20Security%20of%20US%20Critical%20Electric%20Infrastructure%2004202021.pdf.

[64] DOE, *Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats*, April 20, 2021, https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0.

[65] SolarWinds Worldwide LLC, *About SolarWinds*, 2021, https://www.solarwinds.com/company/home.

[66] Isabella Jibilian and Katie Canales, "The US Is Readying Sanctions Against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal," *Business Insider*, April 15, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[67] The malware was later "called Solorigate by Microsoft or SUNBURST by FireEye." Christopher Budd, "Microsoft Unleashes 'Death Star' on SolarWinds Hackers in Extraordinary Response to Breach," *GeekWire*, December 16, 2020, https://www.geekwire.com/2020/microsoft-unleashes-death-star-solarwinds-hackers-extraordinary-response-breach/.

information technology systems, which hackers then used to install even more malware that helped them spy on companies and organizations," and SolarWinds unknowingly sent out the comprised software to customers in updates to its system.[68]

The attack on the Orion system probably began early in 2020, and was said to have given hackers access to confidential data and proprietary system of SolarWinds customers.[69] SolarWinds acknowledged that "its customers include most of America's Fortune 500 companies, the top 10 U.S. telecommunications providers, all five branches of the U.S. military, the State Department, the National Security Agency, and the Office of President of the United States."[70]

The SolarWinds breach demonstrates how some hackers are prepared to engage in a long-term strategy, using the Sunburst Trojan Horse malware spread via Orion updates to mine information and alter software to infect systems compromised beyond the initial cyberattack. FERC announced it stopped using SolarWinds Orion system out of concerns for "the security of our systems and data."[71]

In July 2021, FERC and NERC staff issued a joint whitepaper describing the major supply chain-related cyber security events and the key actions electric industry stakeholders and vendors should take to secure systems.[72]

Changing Grid Technologies

The resources used to provide electric power are changing, as more renewables (particularly wind power and solar photovoltaics) replace fossil fuel sources on price alone, particularly coal.[73] As these and other resources increase in provision of electricity nationwide, a focus may be how best to secure these resources.

Renewable Energy

According to the U.S. Energy Information Administration (EIA), "[r]enewable energy is energy from sources that are naturally replenishing but flow-limited; renewable resources are virtually inexhaustible in duration but limited in the amount of energy that is available per unit of time."[74] Some observers are concerned that renewable generation facilities may not have the cybersecurity protections of other types of power generation, especially if they operate at voltages outside of the

[68] Isabella Jibilian and Katie Canales, "The US Is Readying Sanctions Against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal," *Business Insider*, April 15, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[69] Christopher Bing et al., "Suspected Russian Hackers Spied on U.S. Treasury Emails—Sources," *Reuters*, December 13, 2020, https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PG?edition-redirect=uk.

[70] Ibid.

[71] Christian Vasquez and Blake Sobczak, "'This Is bad.' Hacking Chaos Engulfs FERC, DOE, Microsoft," *E&E News*, December 18, 2020, https://subscriber.politicopro.com/article/eenews/1063721065.

[72] FERC, *SolarWinds and Related Supply Chain Compromise*, July 7, 2021, https://cms.ferc.gov/media/solarwinds-and-related-supply-chain-compromise-0.

[73] Energy Information Administration, *Renewables Account for Most New U.S. Electricity Generating Capacity in 2021*, January 11, 2021, https://www.eia.gov/todayinenergy/detail.php?id=46416.

[74] U.S. Energy Information Administration, *Renewable Energy Explained*, May 20, 2021, https://www.eia.gov/energyexplained/renewable-sources/.

bulk power system, as some systems may be connected to distribution systems operating at lower voltages.[75]

DOE researchers at the National Renewable Energy Laboratory (NREL) are exploring hardware and software solutions that might build-in a certain level of cybersecurity to devices that connect to the grid. According to NREL,

> From a defense perspective, we have a lot of data on a [distributed energy resource (DER)][76] system that could help to potentially identify attackers, and because a DER system is so much more distributed, we also have many ways of responding.... On the other hand, because traditional bulk power plants are utility-owned, they have the advantage of very robust cyber- and physical security protocols.[77]

In 2020, DOE also initiated the Advanced Research on Integrated Energy Systems (ARIES) platform at NREL.[78] DOE states that ARIES "will allow NREL researchers and the scientific community to address the fundamental challenges of integrated energy systems at scale." The program will research "the impact and get the most value from the millions of new devices—such as electric vehicles, renewable generation, hydrogen, energy storage, and grid-interactive efficient buildings—that are being connected to the grid daily."[79]

Energy Storage

With an increasing amount of renewable capacity entering the grid, the need to optimize the use of these resources may lead to an increased deployment of energy storage technologies. While battery storage of electricity is often discussed for the grid, there are other types of storage including the production of ice, pumped hydropower, heat, chilled water, and electrochemical storage. Each of these technologies has its own applications and challenges.[80] The cost, applicability of the type of storage to the project type, and duration and number of cycles possible for charging and discharging the batteries are among the factors considered. Aside from the ability to store electricity produced from renewables at times of off-peak demand, energy storage also may help to stabilize the grid by balancing the grid to maintain system frequency. Energy storage resources also can foster grid resilience by providing power when extreme weather or other circumstances prevent other power generation resources from operating.[81]

---

[75] Zoya Teirstein, "Hackers Found America's Energy Weak Spot," *Grist*, May 10, 2021, https://grist.org/politics/hackers-found-americas-energy-weak-spot/.

[76] According to NREL, "[Distributed Energy Resources] are resources connected to the distribution system close to the load, such as DPV [distributed photovoltaics], wind, combined heat and power, microgrids, energy storage, microturbines, and diesel generators. Energy efficiency, demand response, and electric vehicles are also sometimes considered DERs [distributed energy resources]." Kelsey Horowitz et al., *An Overview of Distributed Energy Resource (DER) Interconnection: Current Practices and Emerging Solutions*, National Renewable Energy Laboratory, NREL/TP-6A20-72102, April 2019, https://www.nrel.gov/docs/fy19osti/72102.pdf.

[77] National Renewable Energy Laboratory, *New Directions Sharpen NREL's Cybersecurity Research, Protecting Energy Systems Beyond the Grid Edge*, October 29, 2020, https://www.nrel.gov/news/features/2020/new-directions-sharpen-nrels-cybersecurity-research.html.

[78] DOE, *Secretary Brouillette Announces ARIES—A Visionary Energy Research Platform*, August 12, 2020, https://www.energy.gov/articles/secretary-brouillette-announces-aries-visionary-energy-research-platform.

[79] Ibid.

[80] National Renewable Energy Laboratory, *Declining Renewable Costs Drive Focus on Energy Storage*, January 2, 2020, https://www.nrel.gov/news/features/2020/declining-renewable-costs-drive-focus-on-energy-storage.html.

[81] For more information on energy storage. See CRS Report R45980, *Electricity Storage: Applications, Issues, and Technologies*, by Richard J. Campbell.

According to Sandia National Laboratory researchers, energy storage systems (ESSs) are "becoming an essential part of the power grid of the future, making them a potential target for physical and cyberattacks. Large-scale ESSs must include physical security technologies to protect them from adversarial actions that could damage or disable the equipment."[82]

As larger, longer duration ESS are considered for the grid (even systems potentially capable of season-long energy storage resources), the importance of secure ESS may become more essential to ensuring the reliability of the grid. Thus, the security of these systems may become a part of planning for the future of the grid.

> Including security as a fundamental component in energy storage industry culture is paramount, even for early development grid-connected ESS technologies. The experience of related power systems industries shows that ignoring security during the new product development cycle may lead to costly and ineffective security solutions when added in later stages of product development."[83]

Cybersecurity of the Smart Grid

Smart Grid modernization ensues as upgrades to electric power infrastructure are added. Electric power transmission substations are being automated with advanced switching capabilities to enhance current flows and control of the grid. PMU devices also are being added to substations to make time- and location-specific measurements of transmission line voltage, current, and frequency. An example is synchrophasor measurements made on the order of 30 times per second instead of data measured once every two to four seconds by current industrial control systems. PMUs may provide better tools to improve power system reliability.[84]

While these new components may add to the ability to control power flows and enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to cyberattack. Other aspects of Smart Grid systems, such as wireless and two-way communications through internet-connected devices, can also increase cybersecurity vulnerabilities. The potential for a major disruption or widespread damage to the nation's power system from a large-scale cyberattack has increased focus on the cybersecurity of the Smart Grid.[85]

The speed inherent in the Smart Grid's enabling digital technologies may also increase the chances of a successful cyberattack, potentially exceeding the ability of the defensive system and defenders to comprehend the threat and respond appropriately. Such scenarios may become more common as machine-to-machine interfaces enabled by artificial intelligence (AI) are being integrated into cyber defenses. However, AI systems learn from experience and may be of limited use in cybersecurity defenses, as experts believe that AI and machine learning "have both negative and positive effects on cybersecurity. AI algorithms use training data to learn how to respond to different situations…. Artificial intelligence and machine learning can improve security, while at the same time making it easier for cybercriminals to penetrate systems with no human intervention."[86]

---

[82] Jay Johnson, et al., *Physical Security and Cybersecurity of Energy Storage Systems*, Sandia National Laboratory, 2021, https://www.sandia.gov/ess-ssl/wp-content/uploads/2021/01/ESHB_Ch18_Physical-Security_Johnson.pdf.

[83] Ibid.

[84] CRS Report R45156, *The Smart Grid: Status and Outlook*, by Richard J. Campbell.

[85] Ibid.

[86] Eddie Segal, "The Impact of AI on Cybersecurity," *IEEE Computer Society*, 2021, https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity.

Thus, one could envision a scenario where AI may be susceptible to intrusion feints, which may cause systems to protect against false or disguised cyberattacks, potentially allowing an attack focused along another path to continue.[87]

According to a report from the Idaho National Laboratory, modernizing the grid with digital technologies comes with its own set of specialized requirements.

> In particular, the upgrade to the smart grid in the U.S. has required utilities to implement new technical practices to protect a vulnerable combination of communication, IT, and OT as well as protect customer privacy. Smart grid software architecture developed or aided in development by utilities, such as the Secure Common Operating Environment (SCOE), has been used to mesh cyber security with smart grid technologies. Furthermore, the smart grid upgrade will not only require robust cyber security, but will need to integrate physical security—that which provides protection to personnel, hardware, programs, networks, and data from unauthorized physical manipulation.[88]

Federal Actions and Programs to Assist Grid Security

Various agencies including FERC, DOE, DHS, and the National Institute of Standards and Technology, have reporting requirements and/or programs providing cyber and physical security assistance to electric utilities and other critical infrastructure companies. Some of these programs provide industry-wide information for companies to act upon, while other programs assist individual companies.

Cybersecurity Incident Reporting

Reliability Standard CIP-008-5 (Cyber Security—Incident Reporting and Response Planning), had directed that incidents must be reported only if they have compromised or disrupted one or more reliability tasks. In 2018, FERC directed NERC to modify CIP Reliability Standards to improve mandatory reporting of cyber security incidents, including attempts that might facilitate subsequent efforts to harm reliable operation of the nation's bulk electric system. As modified, the new requirements consider the function of a responsible entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems. They also consider the nature of the attempted compromise or successful intrusion when developing the reporting thresholds so that only cyber security incidents meeting a certain threat level are reported.[89]

Cybersecurity Risk Information Sharing Program (CRISP)

According to DOE, the Cybersecurity Risk Information Sharing Program (CRISP) is intended to allow energy sector owners and operators to voluntarily share cyber threat data in near real-time,

[87] CRS Report R45156, *The Smart Grid: Status and Outlook*, by Richard J. Campbell.

[88] Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, INL/EXT-16-40692, August 2016, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

[89] FERC, *FERC Requires Expanded Cyber Security Incident Reporting*, July 19, 2018, https://www.ferc.gov/news-events/news/ferc-requires-expanded-cyber-security-incident-reporting.

analyze this data using U.S. intelligence, and receive machine-to-machine threat alerts and mitigation measures.[90]

A 2018 article reported that CRISP had about 26 participating utilities, but that increasing electric utility subscribership was a goal as greater participation would advance the program's analysis capabilities.[91]

> CRISP participating companies essentially install an information-sharing device (ISD) on their network border, just outside the corporate firewall. 'The ISD collects data and sends the data in encrypted form to the CRISP Analysis Center. The Center analyzes the data it receives and, using government-furnished information, sends alerts and mitigation measures back to the participating companies about potential malicious activity.'[92]

In 2020, NERC announced that the Electricity Information Sharing and Analysis Center partnered with DOE to expand CRISP to include Operational Technology. Two pilot programs were established to "identify potential cyber threats to utilities' industrial control systems by capturing raw and/or refined operational technology data and comparing it to CRISP information technology data."[93]

Cybersecurity Capability Maturity Model

In 2021, DOE released version 2.0 of the Cybersecurity Capability Maturity Model (C2M2), a tool designed to help companies of all types and sizes evaluate and improve their cybersecurity capabilities. According to DOE, the C2M2 "updates address the evolving cyber threat and technology landscape,"[94] and was a part of a 100-day plan announced by the Biden Administration in April 2021 to confront cyber threats to critical systems essential to U.S. national and economic security.

Originally released in 2012, the C2M2 is designed to help organizations in the energy sector understand cyber risks to their IT and OT systems. The updated model includes inputs from 145 cybersecurity experts representing 77 energy sector organizations. "Updates address new technologies like cloud, mobile, and artificial intelligence, and evolving threats such as ransomware and supply chain risks, and ultimately support companies in strengthening their operational resilience," according to DOE.[95]

NIST Cybersecurity Framework and FERC-NERC CIP Requirements

In December 2020, FERC began to explore incentives to jurisdictional utilities to improve their cybersecurity.[96] The notice of proposed rulemaking was initiated partly due to questions on

---

[90] DOE, *Cybersecurity Risk Information Sharing Program*, September 2018, https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf.

[91] Sonal Patel, "DOE Lays Out How Power Sector Could Win the Cybersecurity Battle," *POWER Magazine*, May 17, 2018, https://www.powermag.com/doe-lays-out-how-power-sector-could-win-the-cybersecurity-battle/.

[92] Ibid.

[93] NERC, *E-ISAC Expands Key Cybersecurity Program*, November 30, 2020, https://www.nerc.com/news/Pages/E-ISAC-Expands-Key-Cybersecurity-Program.aspx.

[94] DOE, *Department of Energy Releases Updated Cybersecurity Capability Maturity Model*, July 22, 2021, https://www.energy.gov/ceser/articles/department-energy-releases-updated-cybersecurity-capability-maturity-model.

[95] Ibid.

[96] FERC, *FERC Proposes Incentives for Cybersecurity Investments by Public Utilities*, Docket No. RM21-3-000,

whether the current CIP standards can keep up with evolving cybersecurity threats to the grid.[97] Another impetus was a FERC staff whitepaper that discussed rate incentives to align with NIST's Cybersecurity Framework.

> In a June 2020 white paper, Commission staff sought comment on an incentive-based framework that could encourage public utilities to adopt best practices to protect their own transmission systems and improve the security of the grid. Such a framework would allow the electric industry to be more agile in monitoring and responding to new and evolving cybersecurity threats, to identify and respond to a wider range of threats, and to address threats with comprehensive and more effective solutions.
>
> The proposed rule would allow public utilities to seek Commission approval, pursuant to section 205 of the Federal Power Act, of two types of incentives for cybersecurity investments: a rate of return (ROE) adder of 200 basis points or deferred cost recovery for certain cybersecurity-related expenses. Qualifying expenditures would be eligible for either, but not both, incentives. The total cybersecurity incentives requested would be capped at the zone of reasonableness. [98]

According to FERC, the incentives would be available for certain investments that voluntarily apply specific CIP Reliability Standards to facilities that are not subject to those requirements. Incentives also would be available to those companies implementing standards and guidelines from NIST's voluntary framework for improving CI cybersecurity. However, public utilities seeking to implement the proposed incentives would be required to obtain prior Commission approval, and the proposed rule would impose initial and annual reporting requirements.

DOE also supported FERC's proposal to incentivize the cybersecurity of networks in power grid industrial control systems, stating that it "encourages FERC to include incentives to accelerate the development and deployment of (high-fidelity) sensor-based continuous network monitoring cybersecurity capabilities for operating the transmission system (e.g., operational technology) in its framework of incentives."[99]

NIST Recommendations and Industry Best Practices

The FERC staff whitepaper also discussed broadening FERC-NERC CIP requirements to align with NIST's Cybersecurity Framework.[100] FERC staff recognized that some NIST cyber framework recommendations address areas of cybersecurity not covered by CIP standards. Examples included

> An installation of a dynamic asset management program to improve a utility's ability to quickly detect and address new or previously unknown equipment on its network….
>
> Implementing a process that automatically and continuously scans the current inventory of hardware and software across both the information technology and operational technology networks can identify and block any unauthorized access. This is an enhancement that is not currently covered by the CIP Reliability Standards….

December 17, 2020, https://www.ferc.gov/news-events/news/ferc-proposes-incentives-cybersecurity-investments-public-utilities.

[97] 173 FERC ¶ 61,240.

[98] Ibid.

[99] DOE, Cybersecurity Incentives Policy White Paper, Docket No. AD20-19-000, August 27, 2020, https://elibrary.ferc.gov/eLibrary/filelist?document_id=14886986&amp.

[100] FERC, *Cybersecurity Incentives Policy White Paper*, June 18, 2020, https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf.

> Another example that may be applicable under the identified NIST Framework security control type of automated and continuous monitoring would be implementation of a dynamic file analysis program or a "sandbox." … In simple terms, a sandbox is an isolated environment that mimics the end-user operating environment. Any malicious code deployed in the sandbox will be activated when placed there, but it will be isolated from the information technology and operational technology networks, thereby protecting the networks while alerting the utility to the threat. The deployment of sandboxes enhances the ability of a utility to detect and prevent the delivery of malicious code, disrupt social engineering attacks on users, test software for dangerous behavior, and perform post-incident forensic triage and analysis. Putting this added layer of protection in place is an enhancement that is not required by the CIP Reliability Standards but is recommended by the NIST Framework and could offer cybersecurity benefits to the transmission system.[101]

In a statement submitted to the House Energy and Commerce Committee, a FERC official also affirmed the agency's support for utilities to also follow industry "best practices."

> [FERC's Office of Energy Infrastructure Security (OEIS)] partners with other federal agencies, states, and industry to develop and promote best practices for critical energy infrastructure security. Working with these entities, OEIS helps identify new and emerging threats, inform the private sector of them, performs voluntary cybersecurity evaluations, and assists with mitigating actions. For example, OEIS conducts voluntary architecture assessments of interested Commission-jurisdictional utilities' computer networks that control the operations of their facilities. Conducted onsite, these assessments are specific to the organization, reviewing everything from the configuration of legacy equipment to the application of state-of-the-art protection systems. Another example is that OEIS works with the Office of Director of National Intelligence, specifically the National Counterintelligence and Security Center, to conduct briefings and exchange information with state and industry officials about the current threats industry is facing and what can be done to address them.[102]

Performance Goals for Electric Utilities

Voluntary cybersecurity "performance goals" were proposed by the Biden Administration for critical infrastructure companies.

> Pursuant to section 7(d) of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), the Secretary of Homeland Security, in coordination with the Secretary of Commerce (through the Director of the National Institute of Standards and Technology) and other agencies, as appropriate, shall develop and issue cybersecurity performance goals for critical infrastructure to further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety.[103]

In September 2021, CISA issued preliminary cross-sector cybersecurity performance goals and objectives for critical infrastructure control systems. The performance goals were developed in concert with NIST, and address nine main categories covering "specific objectives that support

[101] Ibid.

[102] U.S. Congress, House Oversight and Reform, Subcommittee on National Security, *Defending the U.S. Electric Grid Against Cyber Threat*, Testimony of Joseph McClelland, FERC Director, Office of Energy Infrastructure Security, July 27, 2021.

[103] The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* , July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

the deployment and operation of secure control systems that are further organized into baseline and enhanced objectives."[104]

According to one report, developing clear performance goals will help to develop "actionable items for bulk electric system security and all sectors," while observing that "sector-specific" performance goals should not preclude learning how other sectors have approached cybersecurity.[105]

Improving Cybersecurity of Distribution and Smaller Utilities

Mandatory CIP requirements for bulk power system do not apply to most distribution utilities that sell electricity directly to customers for their own use, or to many rural electric cooperatives. Since financial resources at smaller utilities are often limited, the emphasis of cybersecurity is often on managing risk. The NIST Cybersecurity Framework provides information that smaller utilities can use to help them secure their systems, and the trade association's for public power and electric cooperatives provide cybersecurity tools to assist their membership.

For example, the National Rural Electric Cooperative Association (NRECA) has the Essence Technology program, which NRECA describes as an "anomaly-detection platform that uses operational technology sensors to identify and warn of possible network breaches in real time."[106] NRECA states that this allows them to "share their anonymized cybersecurity and threat data with trusted government partners."[107] The platform has been further developed with subsequent funding from DOE and the Pacific Northwest National Laboratory.[108]

CISA provides free assistance to critical infrastructure companies to improve cybersecurity within their organizations. CISA describes this assistance as helping critical infrastructure organizations assess, identify, and reduce their exposure to cybersecurity threats, including ransomware.[109]

Additional Actions to Potentially Improve Grid Cybersecurity

Multi-Factor Authentication

Among the most basic actions utilities can take to improve security is the adoption of multi-factor authentication (MFA) for access to IT systems. MFA is a security practice that requires multiple

[104] CISA, *Critical Infrastructure Control Systems Cybersecurity Performance Goals and Objectives*, September 22, 2021, https://www.cisa.gov/control-systems-goals-and-objectives.

[105] Robert Walton, "Biden Orders Voluntary Cybersecurity Performance Goals for Electric Utilities, Other Critical Sectors," *UtilityDive*, July 29, 2021, https://www.utilitydive.com/news/biden-orders-voluntary-cybersecurity-performance-goals-for-electric-utiliti/604115/.

[106] National Rural Electric Cooperative Association, *Fact Sheet: Essence 2.0 Cybersecurity Technology*, April 2, 2021, https://www.electric.coop/wp-content/uploads/2021/04/NRECA_Essence_2-pager-033121.pdf.

[107] Ibid.

[108] NRECA, "NRECA Awarded $3.9 Million for Cybersecurity Information Sharing Partnership," May 10, 2021, https://www.electric.coop/nreca-awarded-3-9-million-for-cybersecurity-information-sharing-partnership.

[109] DHS-CISA, *Cyber Hygiene Services*, 2021, https://www.cisa.gov/cyber-hygiene-services.

credentials to verify a user's identity, requiring credentials from at least two of three categories instead of just a username and password.[110] These categories include user-known data such as a personal identification number or password, user-possessed equipment such as a smartphone or smart card, or user-identifiable characteristics (i.e., biometric data) such as fingerprints or voice recognition. "If two categories of authentication are used, the process is called two-factor authentication (2FA). If three are used, the method is referred to as 3FA or three-factor authentication. Both 2FA and 3FA are subsets of MFA."[111]

However, according to one article from IDG Communications, MFA can embody both the best and worst of business IT security practices. [112]

> [W]hen MFA is done well it can be effective, but when IT managers take shortcuts it can be a disaster. And while more businesses are using more MFA methods to protect user logins, it still is far from universal. Indeed, according to a survey conducted by Microsoft last year, 99.9% of compromised accounts did not use MFA at all and only 11% of enterprise accounts are protected by some MFA method.[113]

MFA implementation can be complicated, but following poor practices to accommodate users can subvert MFA security. For example, an employee may use MFA for account access, but accessing the account also requires a secondary or tertiary account access method (e.g., when they contact a help desk). If those secondary or tertiary methods of verifying the account are not equally secure, opportunities could arise for malicious account access.

Separate and Independent OT Networks

IT/OT convergence has been driven by the potential for better control of the utility power production and transmission processes, and easier remote analysis of data via the internet. This may improve efficiency and "decision-making, as they have access to real-time insights that the data provides."[114] However, for good cyber hygiene, CISA recommends implementing robust segmentation between IT and OT networks, and implementing a continuous and vigilant system-monitoring program.[115]

Preparation and Practice for Potential Intrusions

As was demonstrated by the Colonial Pipeline ransomware attack,[116] an intrusion into a company's IT network can threaten an OT network. CISA has recommendations for the steps organizations should take to improve their resilience against ransomware attacks.

---

[110] Justin Sheil, "How Important is MFA for Remote Work?," *Electric*, July 30, 2020, https://www.electric.ai/blog/how-important-is-mfa-for-remote-work.

[111] Ibid.

[112] David Strom, *How to Hack 2FA: 5 Attack Methods Explained*, IDG Communications CSO, June 3, 2021, https://www.csoonline.com/article/3620223/how-to-hack-2fa.html.

[113] Ibid.

[114] Stephen Bigelow and Ben Lutkevich, "What Is IT/OT Convergence? Everything You Need to Know," TechTarget, 2020, https://searchitoperations.techtarget.com/definition/IT-OT-convergence.

[115] Cybersecurity and Infrastructure Security Agency, *Rising Ransomware Threat to Operational Technology Assets*, June 2021, https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf.

[116] For more information on the Colonial Pipeline ransomware attach, see CRS Insight IN11667, *Colonial Pipeline: The DarkSide Strikes*, by Paul W. Parfomak and Chris Jaikaran.

> When it comes to responding to ransomware attacks that may impact ICS, [CISA] recommends a series of steps that include determining which systems are impacted and isolating them, disconnecting or shutting down impacted devices to prevent the ransomware from spreading, triaging affected systems for restoration and recovery, conducting an initial investigation, and engaging internal and external parties (including CISA) for assistance.
>
> If none of the initial mitigation actions appear possible, CISA recommends collecting system images, memory dumps and other digital evidence, and consulting law enforcement to find out if a decryptor is available for the ransomware that targeted them.[117]

Considering Best Practices from Other Sectors

In a 2020 article, McKinsey Company analysts identified three characteristics that make the power sector especially vulnerable to cyberthreats:

- an increasing number of cyber threats to utilities from nation-state actors that seek to cause security and economic dislocation,
- the "expansive and increasing attack surface" of electric and gas utilities, arising from their geographic and organizational complexity, including the decentralized nature of many organizations' cybersecurity leadership, and
- the electric-power and gas sector's unique interdependencies between physical and cyber infrastructure make companies vulnerable to exploitation, including billing fraud with wireless "smart meters," the commandeering of OT systems to stop multiple wind turbines, and even physical destruction.

The article discussed cybersecurity practices in banking and the federal government that could be applicable to energy companies, including engaging in industry-wide collaboration.[118] The article also recommended actions related to improving the organizational focus on security, among which were[119]

- developing strategic threat intelligence that is relevant to the company leadership: Lead intelligence reporting with the potential business impact of threats. Integrate intelligence reporting into strategic planning and war-gaming,
- integrating security across regions and organizations: Create a common operating picture across physical security, cybersecurity, and IT. Design clear and safe separation between IT and OT network according to a defined set of rules. IT and OT organizations should maintain their own firewalls at the edge, but firewall policies should be coordinated to ensure that both organizations have access to requisite functions and data on the other's networks, and,
- partnering across the industry: Create common standards, and use industry organizations to push for security by design in IT and OT technologies, especially smart-grid devices that may lie outside utilities' direct control. Participate in regional consortiums to discuss security across shared power grids

[117] Eduard Kovacs, "CISA Warns of Threat Posed by Ransomware to Industrial Systems," *Security Week*, June 14, 2021, https://www.securityweek.com/cisa-warns-threat-posed-ransomware-industrial-systems.

[118] Tucker Bailey, Adam Maruyama, and Daniel Wallance, "The Energy-Sector Threat: How to Address Cybersecurity Vulnerabilities," *Power Magazine*, October 9, 2020, https://www.powermag.com/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities/.

[119] Ibid.

and ensure secure implementations of OT protocols (such as International Electrotechnical Commission standards) from utility to utility.

117th Congress Legislation

The Enhancing Grid Security through Public-Private Partnerships Act (H.R. 2931), as passed by the House on July 19, 2021, would direct DOE to implement a program to facilitate and encourage public-private partnerships to address and mitigate the physical security and cybersecurity risks of electric utilities. In carrying out the program, DOE would be required to take into consideration different sizes of electric utilities and the regions that such utilities serve, prioritize electric utilities with fewer available resources due to size or region, and utilize and leverage existing DOE programs.

The Infrastructure Investment and Jobs Act, (H.R. 3684), was passed by the House and Senate then returned to the House for further consideration. Most recent debate occurred in the House on October 1, 2021. Division D—Energy of the bill contains Subtitle B—Cybersecurity, which has sections that would address electric grid security through the use of public-private partnerships, cyber sense programs, FERC incentives for cybersecurity improvements and data sharing about potential security threats, and assistance and grants to rural and municipal utilities, among other provisions.

The Cyber Sense Act of 2020 (S. 2199), introduced on June 23, 2021, would require the Secretary of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, among other purposes.

The Protect American Power Infrastructure Act (S. 2269), introduced on June 24, 2021, would prohibit any person who is the owner or operator of defense critical electric infrastructure from engaging in any transaction relating to that defense critical electric infrastructure that involves any covered equipment in which a foreign adversary has an ownership or any other interest. The bill would address foreign adversary ownership through an interest in a contract for the provision of the covered equipment, over which a foreign adversary has control, or exercises influence.

The Cyber Incident Notification Act of 2021 (S. 2407), introduced on July 21, 2021, would require federal government agencies, federal contractors, and critical infrastructure operators to notify CISA when a security breach is detected. The bill would allow the U.S. government to mobilize to protect critical industries, among other actions. The bill also would grant legal immunity to organizations that come forward with breach reports.

Issues for Congress

The electric power industry does not have the intelligence-gathering capabilities to deal with the many cyber and physical threats to the grid, many of which appear to come from actors abroad. Instead, the U.S. government analyzes all-source intelligence to understand threats to the energy grid and shares that information with the electricity industry, which applies its expertise to understanding the risks posed to the grid. Government information that is timely and relevant as to the severity of a threat to the grid, and which contains whether a need exists for immediate action is helpful to the electricity industry. Congress may investigate how best to ensure that intelligence information on grid cyberthreats can be better disseminated and on a timelier basis.

The bulk electric system is subject to mandatory and enforceable critical infrastructure protection rules for cyber and physical security under the FERC's reliability mandate. However, the energy

sector is one of 16 critical infrastructure sectors identified by DHS.[120] Given that the grid relies on several of the other sectors (for example, the water and transportation sectors), the question of whether these other sectors should also have similar, mandatory standards focused on support of the electric power sector may be an issue for Congress to consider.

The electric power system in the United States is evolving, but not consistently across sectors and regions of the country. Some may assert that such inconsistencies could add a level of complexity that may make a nationwide cyber event more unlikely. However, the development of a modern electric power system could foster the prospects of U.S. economic health and competitiveness. Policy options designed to ensure that the developing electric power system is as secure as possible are likely to be a consideration for Congress.

Author Information

Richard J. Campbell
Specialist in Energy Policy

[120] Cybersecurity and Infrastructure Security Agency, *Critical Infrastructure Sectors*, 2021, https://www.cisa.gov/critical-infrastructure-sectors.

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.